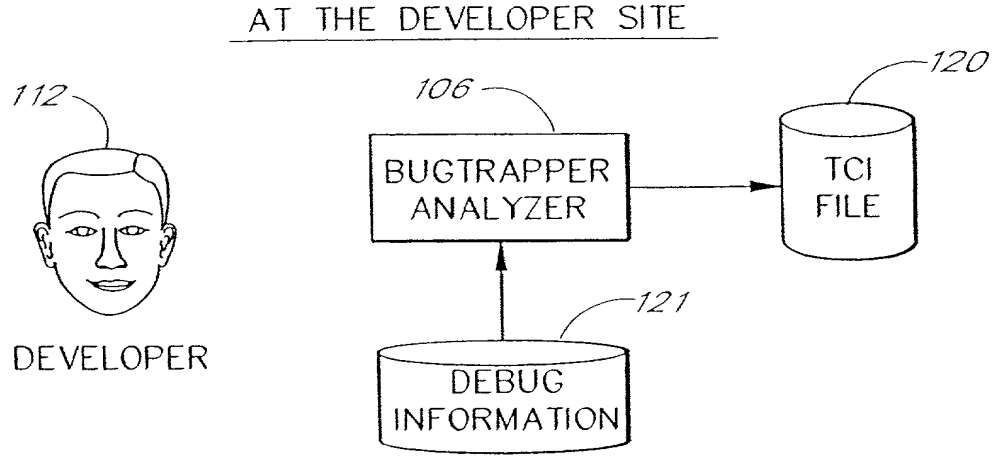

AT THE DEVELOPER SITE
112
106
120
BUGTRAPPER ANALYZER
TCI FILE
DEVELOPER
121
DEBUG INFORMATION

FIG. 1A

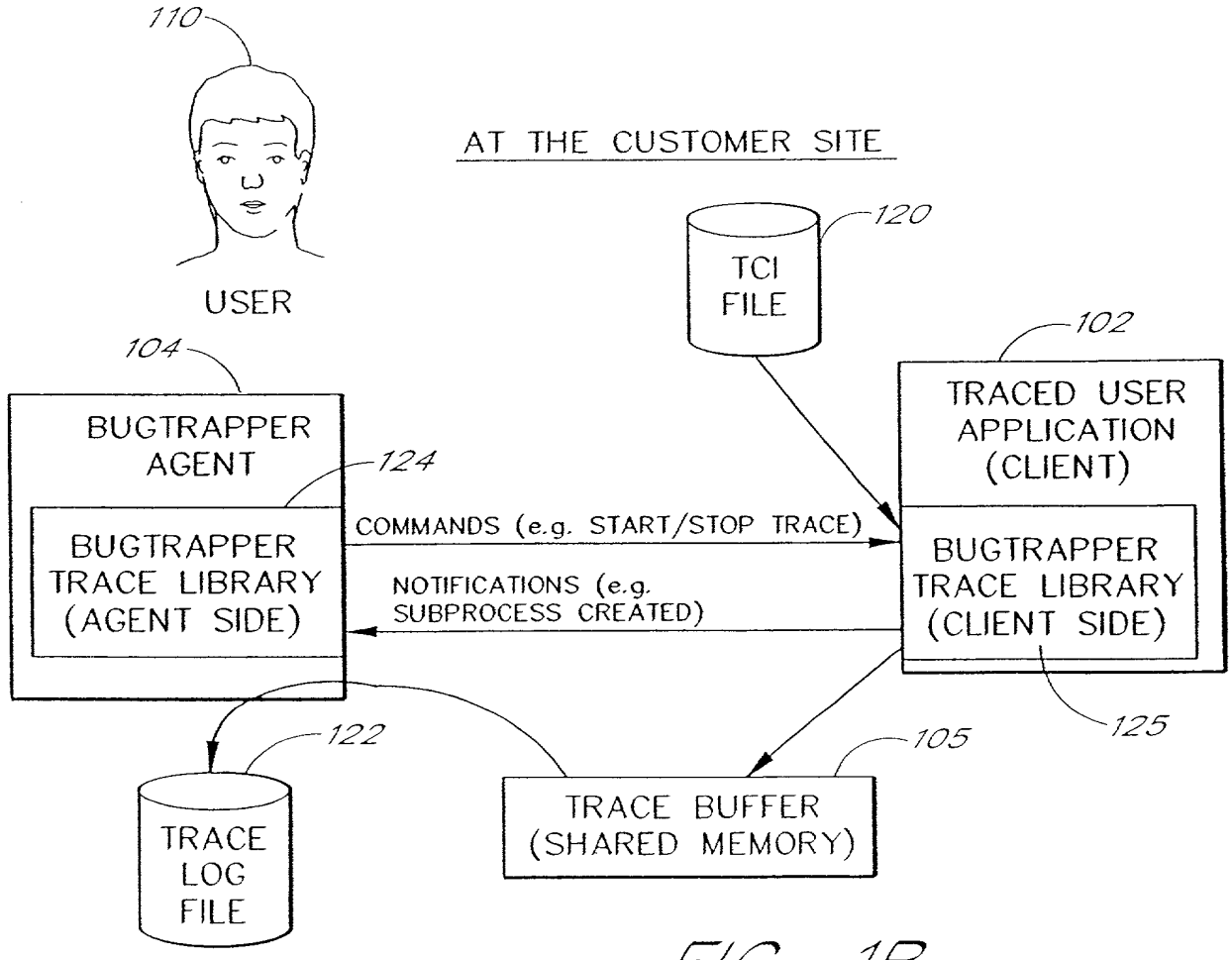

110
AT THE CUSTOMER SITE
120
TCI FILE
USER
102
104
TRACED USER APPLICATION (CLIENT)
BUGTRAPPER AGENT
124
BUGTRAPPER TRACE LIBRARY (AGENT SIDE)
COMMANDS (e.g. START/STOP TRACE)
NOTIFICATIONS (e.g. SUBPROCESS CREATED)
BUGTRAPPER TRACE LIBRARY (CLIENT SIDE)
125
122
105
TRACE LOG FILE
TRACE BUFFER (SHARED MEMORY)

FIG. 1B

20162.0012.2004.2004

BACK AT THE DEVELOPER'S SITE

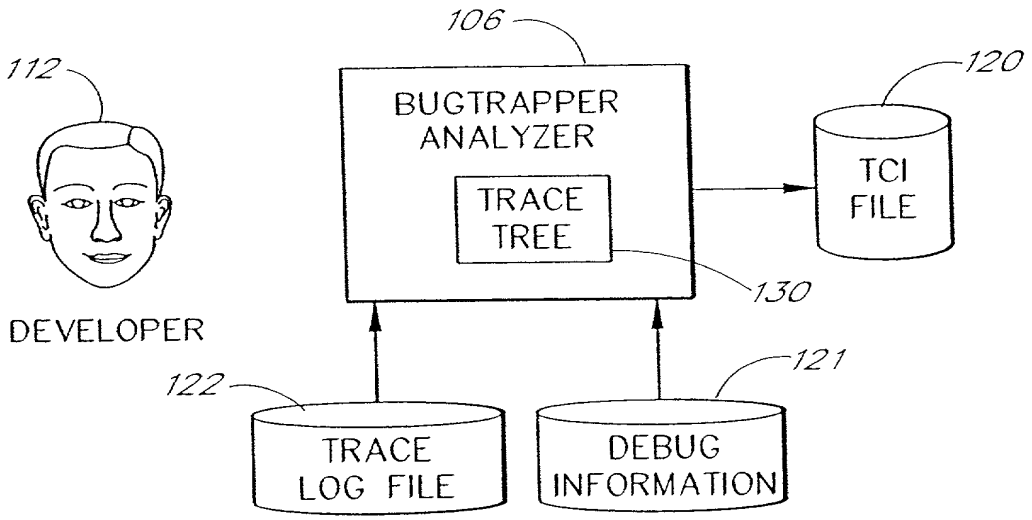


FIG. 1C

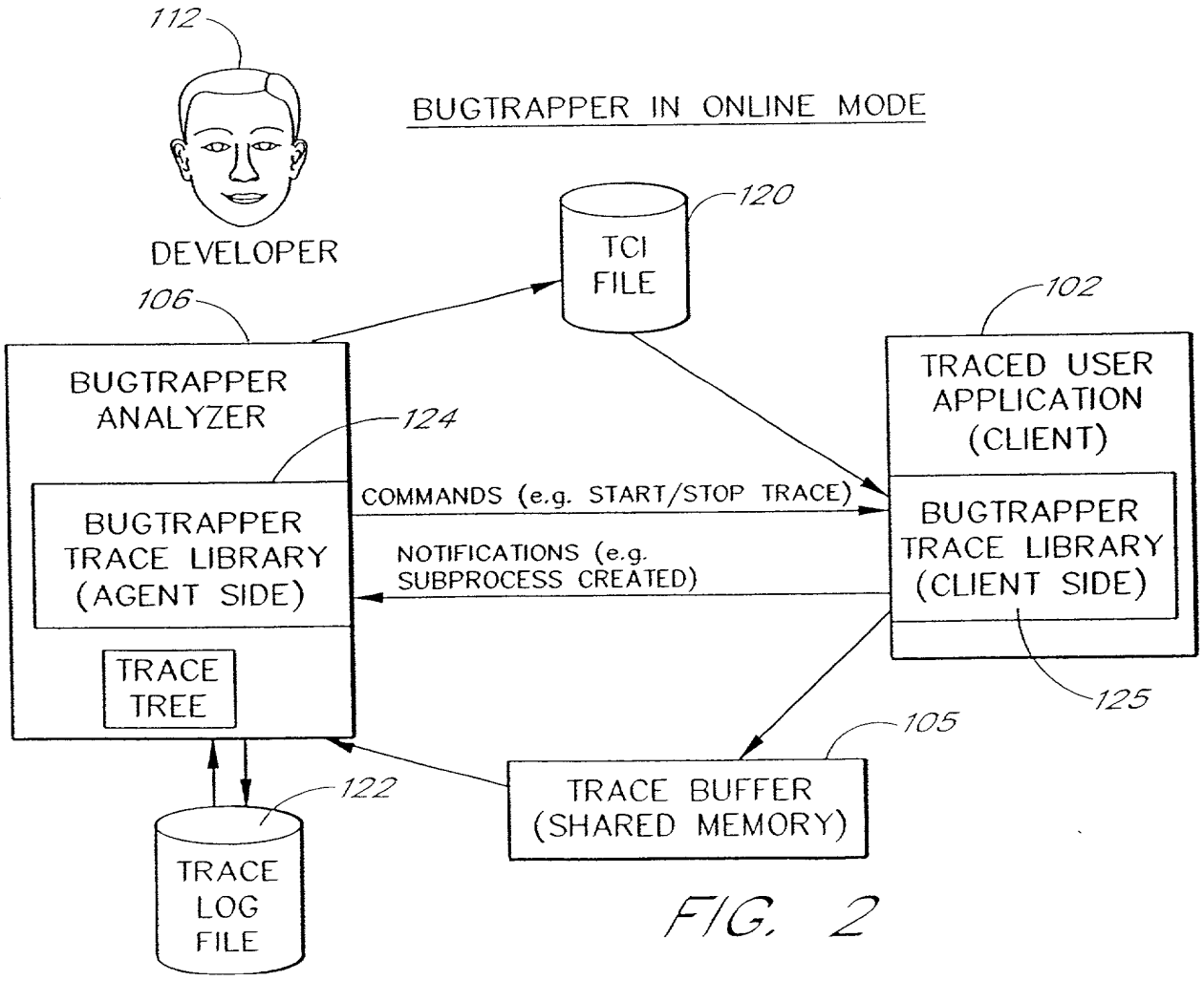


FIG. 2

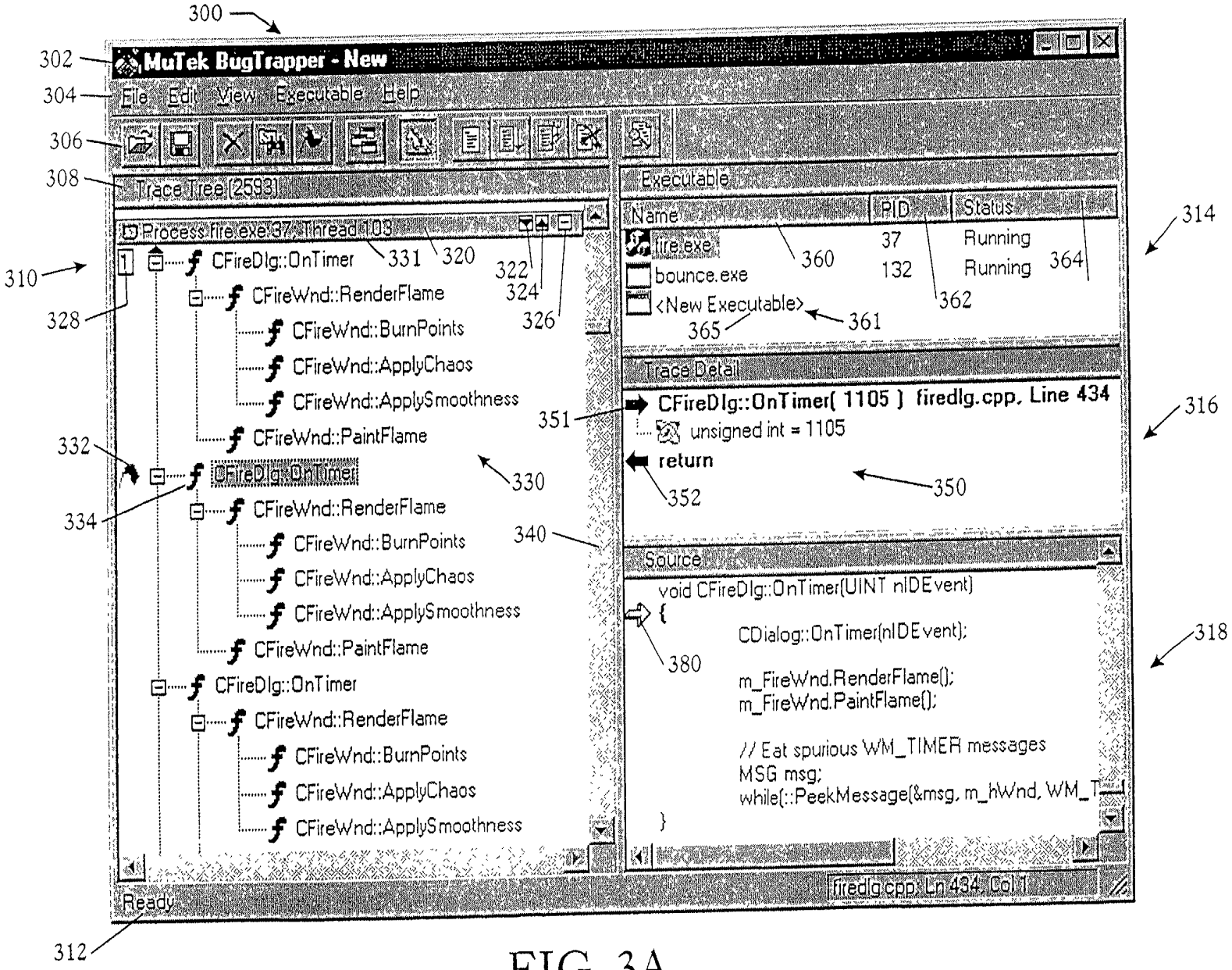

300
302
MuTek BugTrapper - New
304
File Edit View Executable Help
306
308
Trace Tree [2593]
Process fire.exe 37, Thread 103
310
328
CFireDlg::OnTimer
331
320
322
324
326
CFireWnd::RenderFlame
CFireWnd::BurnPoints
CFireWnd::ApplyChaos
CFireWnd::ApplySmoothness
CFireWnd::PaintFlame
332
334
CFireDlg::OnTimer
330
CFireWnd::RenderFlame
CFireWnd::BurnPoints
CFireWnd::ApplyChaos
CFireWnd::ApplySmoothness
CFireWnd::PaintFlame
CFireDlg::OnTimer
CFireWnd::RenderFlame
CFireWnd::BurnPoints
CFireWnd::ApplyChaos
CFireWnd::ApplySmoothness
340
Executable
Name
PID
Status
314
fire.exe
37
Running
360
364
bounce.exe
132
Running
362
<New Executable>
365
361
Trace Detail
351
CFireDlg::OnTimer(1105) firedlg.cpp, Line 434
unsigned int = 1105
return
352
350
316
Source
void CFireDlg::OnTimer(UINT nIDEvent)
{
380
CDialog::OnTimer(nIDEvent);
m_FireWnd.RenderFlame();
m_FireWnd.PaintFlame();
// Eat spurious WM_TIMER messages
MSG msg;
while(::PeekMessage(&msg, m_hWnd, WM_T
}
318
firedlg.cpp Ln 434 Col 1
Ready
312

FIG. 3A

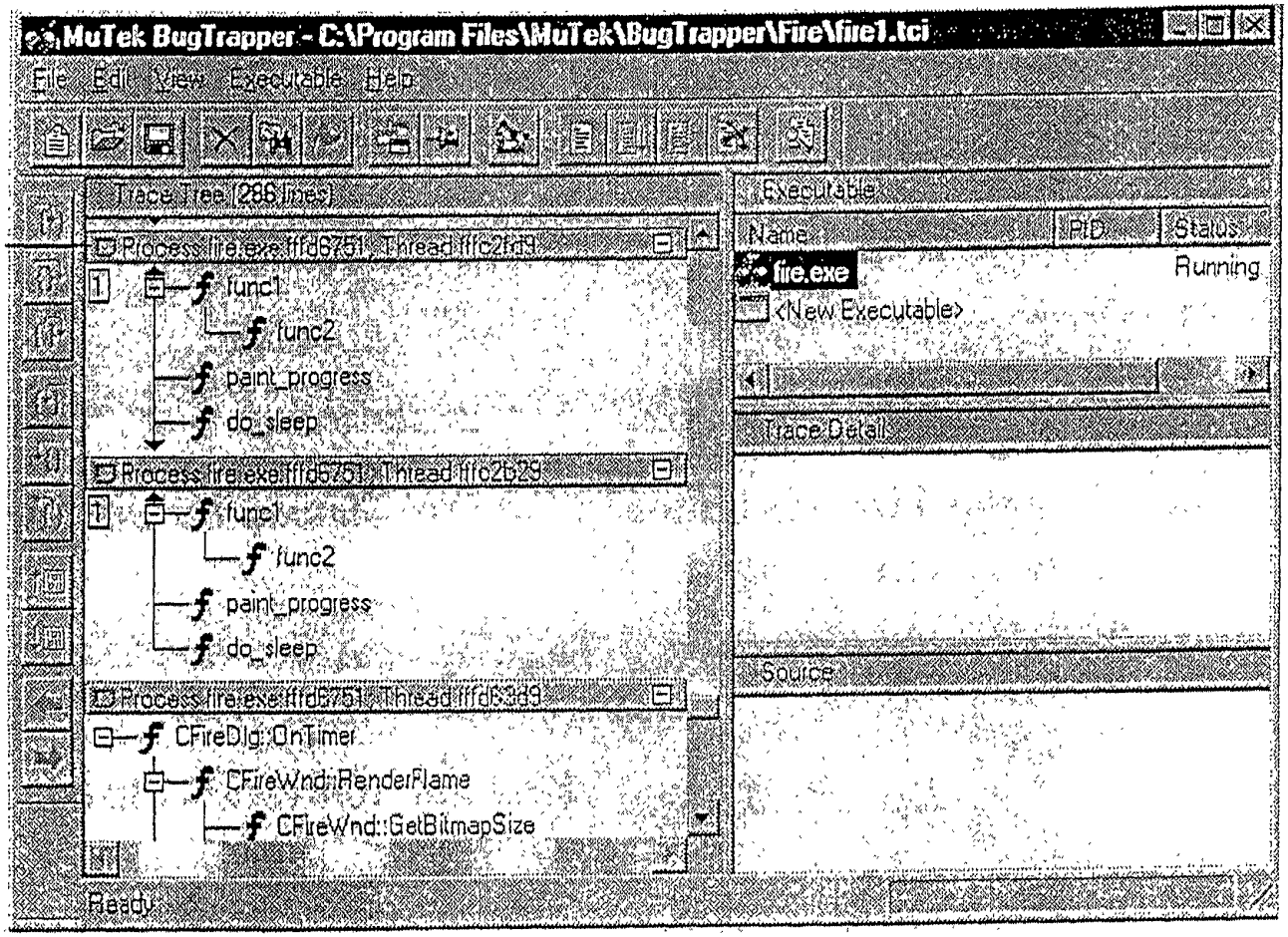

MuTek BugTrapper - C:\Program Files\MuTek\BugTrapper\Fire\fire1.tci
File Edit View Executable Help
Trace Tree (286 lines)
Process fire.exe fffd6751, Thread fffc2fd9
func1
func2
paint_progress
do_sleep
Process fire.exe fffd6751, Thread fffc2b29
func1
func2
paint_progress
do_sleep
Process fire.exe fffd6751, Thread fffd63d9
CFireDlg::OnTimer
CFireWnd::RenderFlame
CFireWnd::GetBitmapSize
Ready
Executable
Name
PID
Status
fire.exe
Running
<New Executable>
Trace Detail
Source

FIG. 3B

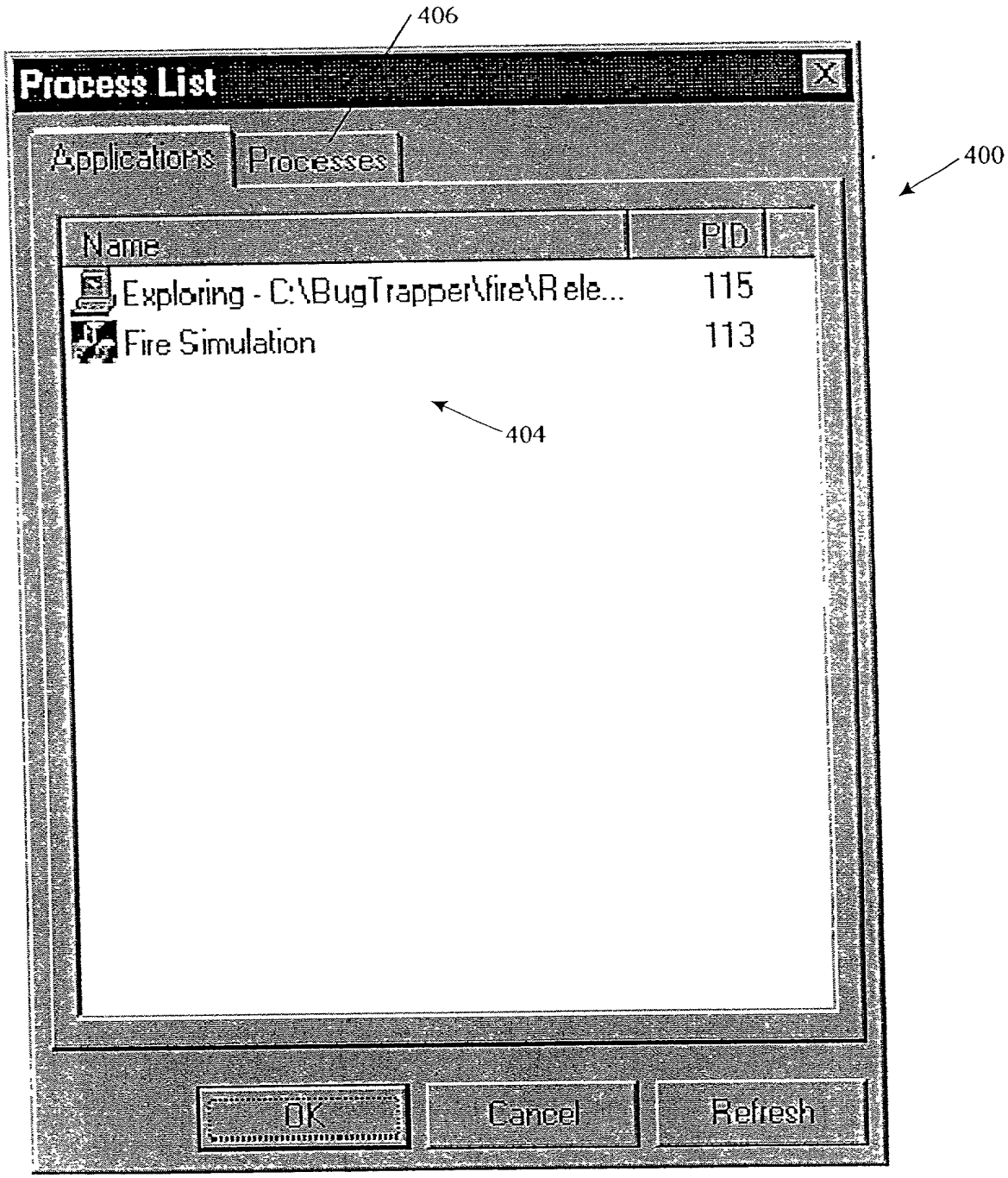

406
Process List
Applications
Processes
400
Name
PID
Exploring - C:\BugTrapper\fire\Rele...
115
Fire Simulation
113
404
OK
Cancel
Refresh

FIG. 4

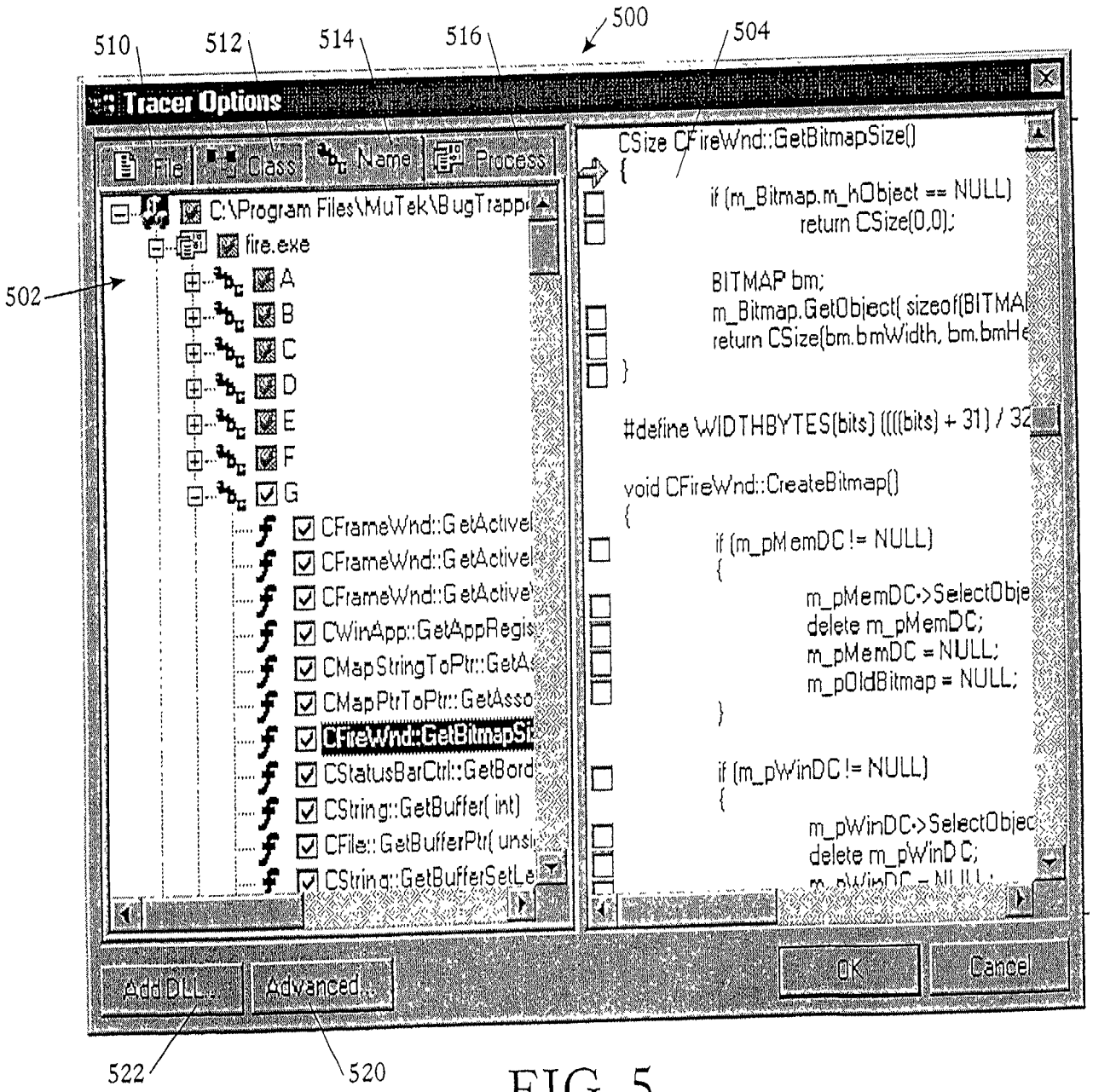

500
510
512
514
516
504
502
Tracer Options
File
Class
Name
Process
C:\Program Files\MuTek\BugTrapp
fire.exe
A
B
C
D
E
F
G
CFrameWnd::GetActivel
CFrameWnd::GetActivel
CFrameWnd::GetActivel
CWinApp::GetAppRegis
CMapStringToPtr::GetA
CMapPtrToPtr::GetAsso
CFireWnd::GetBitmapSi
CStatusBarCtrl::GetBord
CString::GetBuffer(int)
CFile::GetBufferPtr(unsi
CString::GetBufferSetLe
CSize CFireWnd::GetBitmapSize()
{
if (m_Bitmap.m_hObject == NULL)
return CSize(0,0);
BITMAP bm;
m_Bitmap.GetObject(sizeof(BITMA
return CSize(bm.bmWidth, bm.bmHe
}
#define WIDTHBYTES(bits) ((((bits) + 31) / 32
void CFireWnd::CreateBitmap()
{
if (m_pMemDC != NULL)
{
m_pMemDC->SelectObje
delete m_pMemDC;
m_pMemDC = NULL;
m_pOldBitmap = NULL;
}
if (m_pWinDC != NULL)
{
m_pWinDC->SelectObjec
delete m_pWinDC;
Add DLL...
Advanced...
OK
Cancel
522
520

FIG. 5

Exhibit 2003, page 7

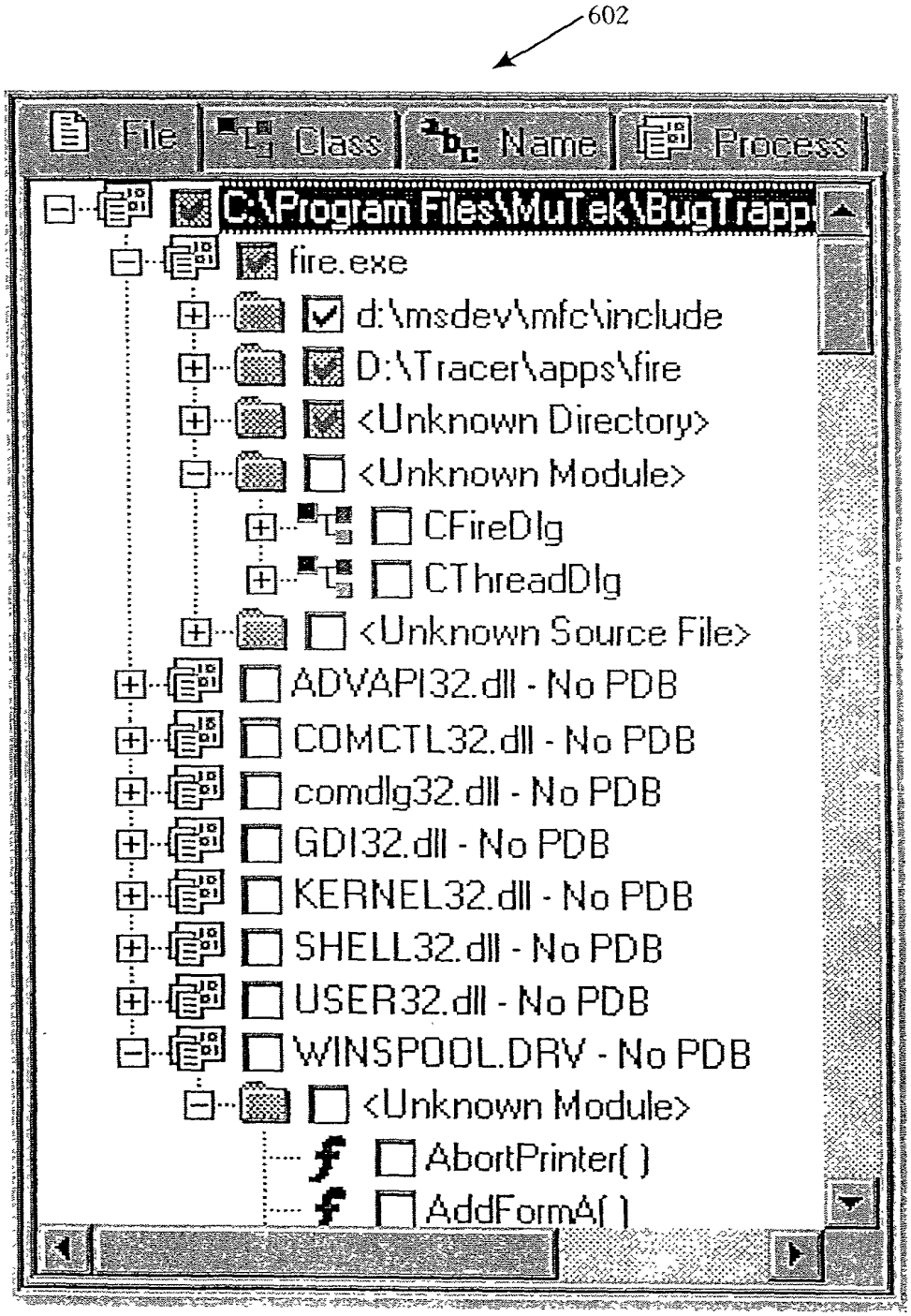


FIG. 6

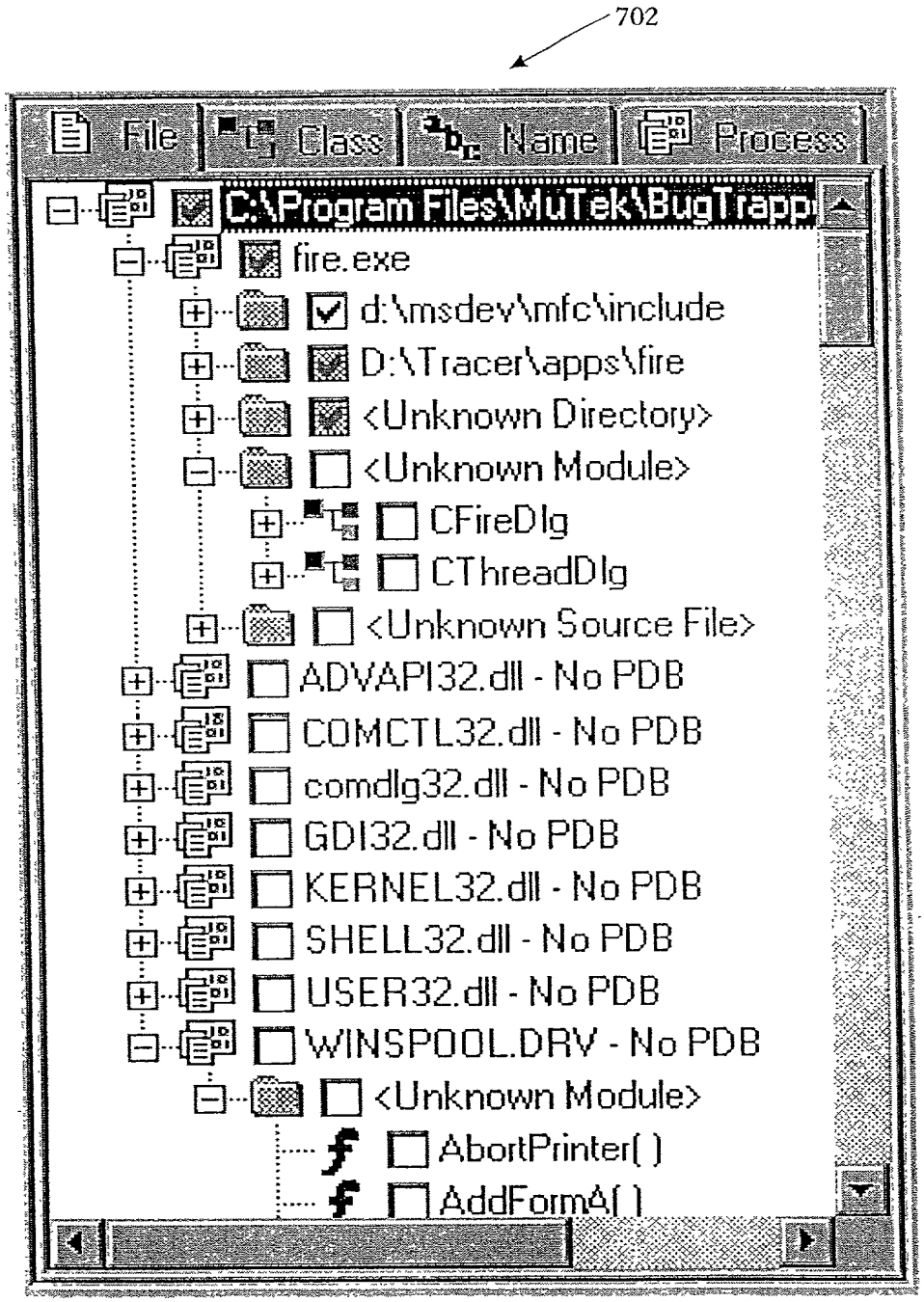

702
File
Class
Name
Process
C:\Program Files\MuTek\BugTrapp
fire.exe
d:\msdev\mfc\include
D:\Tracer\apps\fire
<Unknown Directory>
<Unknown Module>
CFireDlg
CThreadDlg
<Unknown Source File>
ADVAPI32.dll - No PDB
COMCTL32.dll - No PDB
comdlg32.dll - No PDB
GDI32.dll - No PDB
KERNEL32.dll - No PDB
SHELL32.dll - No PDB
USER32.dll - No PDB
WINSPOOL.DRV - No PDB
<Unknown Module>
AbortPrinter( )
AddFormA( )

FIG. 7

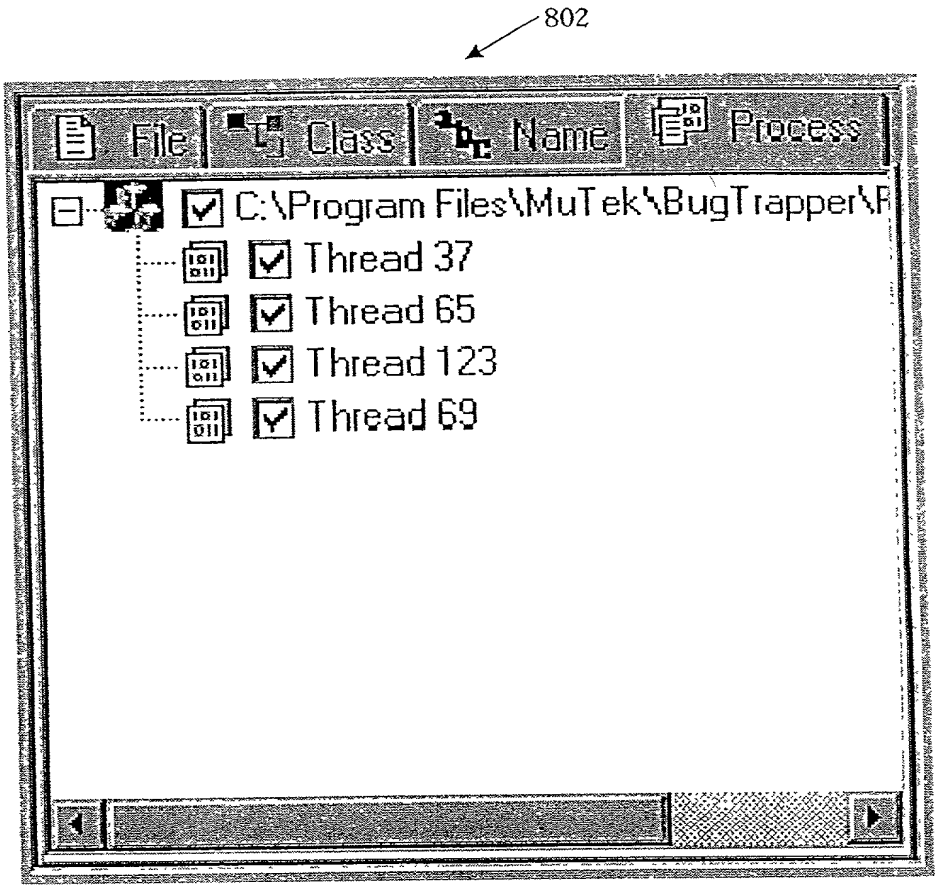

802
File
Class
Name
Process
C:\Program Files\MuTek\BugTrapper\B
Thread 37
Thread 65
Thread 123
Thread 69

FIG. 8

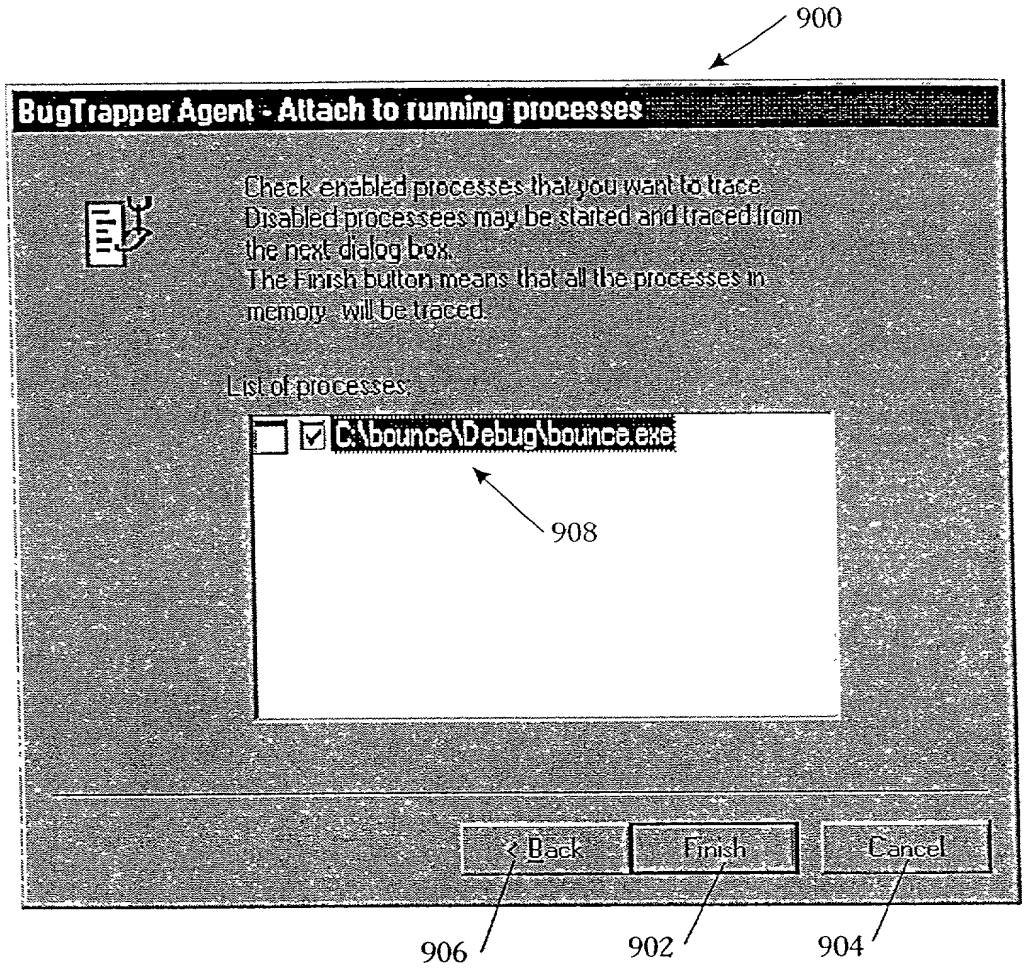

900
BugTrapper Agent - Attach to running processes
Check enabled processes that you want to trace.
Disabled processees may be started and traced from the next dialog box.
The Finish button means that all the processes in memory will be traced.
List of processes:
C:\bounce\Debug\bounce.exe
908
< Back
Finish
Cancel
906
902
904

FIG. 9

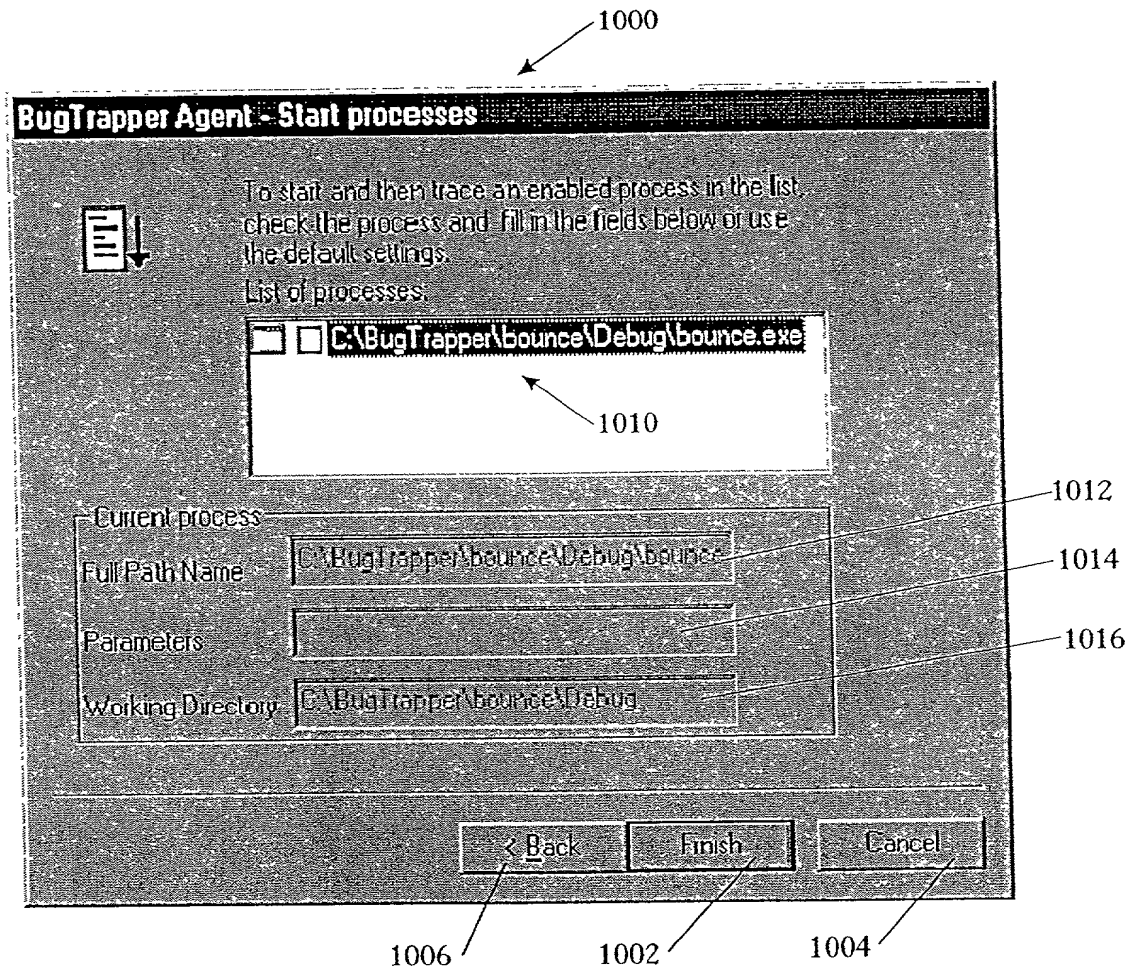

1000
BugTrapper Agent - Start processes
To start and then trace an enabled process in the list, check the process and fill in the fields below or use the default settings.
List of processes:
C:\BugTrapper\bounce\Debug\bounce.exe
1010
Current process
Full Path Name
C:\BugTrapper\bounce\Debug\bounce
1012
Parameters
1014
Working Directory
C:\BugTrapper\bounce\Debug
1016
< Back
Finish
Cancel
1006
1002
1004

FIG. 10

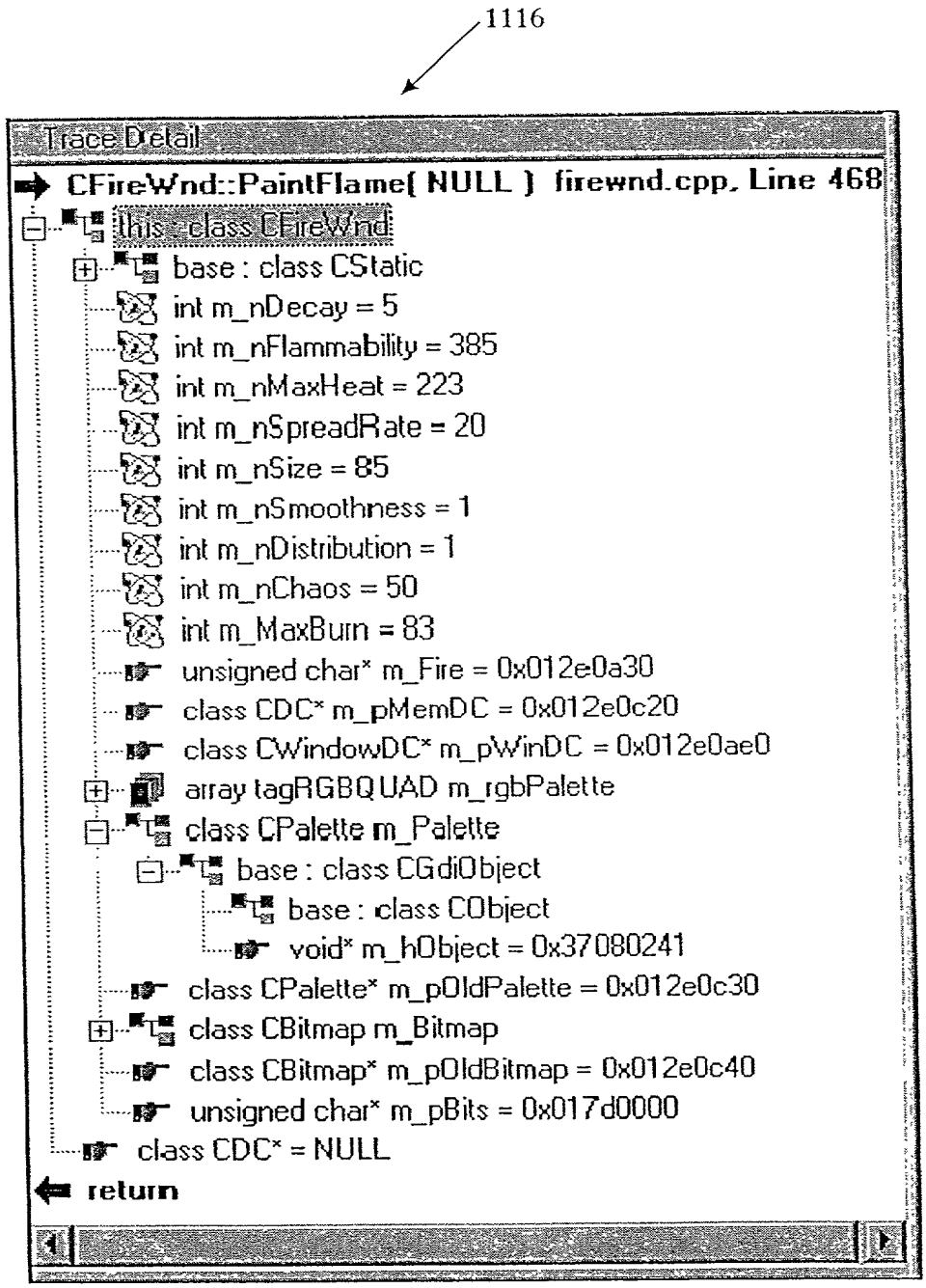

1116
Trace Detail
CFireWnd::PaintFlame(NULL) firewnd.cpp, Line 468
this : class CFireWnd
base : class CStatic
int m_nDecay = 5
int m_nFlammability = 385
int m_nMaxHeat = 223
int m_nSpreadRate = 20
int m_nSize = 85
int m_nSmoothness = 1
int m_nDistribution = 1
int m_nChaos = 50
int m_MaxBurn = 83
unsigned char* m_Fire = 0x012e0a30
class CDC* m_pMemDC = 0x012e0c20
class CWindowDC* m_pWinDC = 0x012e0ae0
array tagRGBQUAD m_rgbPalette
class CPalette m_Palette
base : class CGdiObject
base : class CObject
void* m_hObject = 0x37080241
class CPalette* m_pOldPalette = 0x012e0c30
class CBitmap m_Bitmap
class CBitmap* m_pOldBitmap = 0x012e0c40
unsigned char* m_pBits = 0x017d0000
class CDC* = NULL
return

FIG. 11

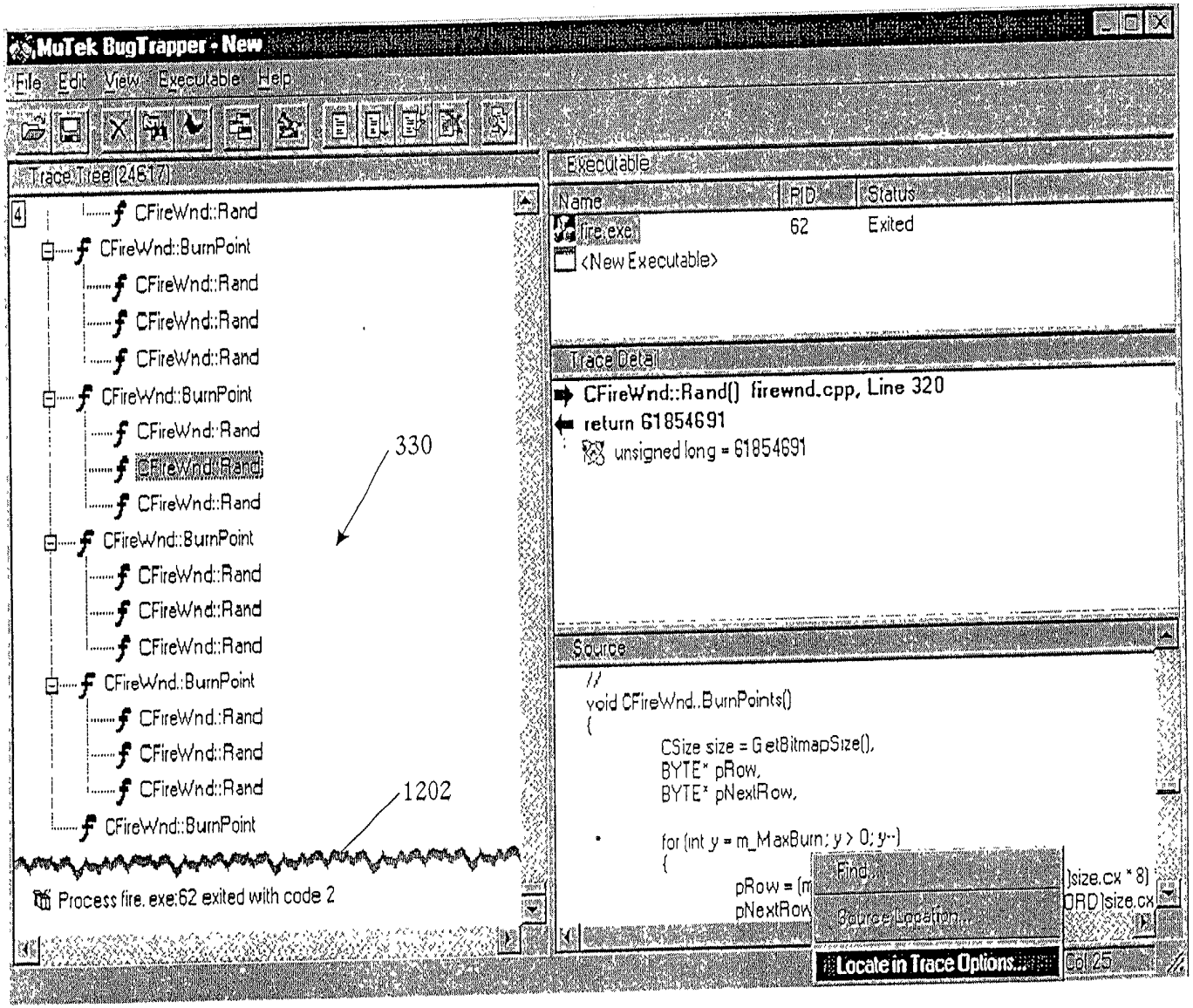

MuTek BugTrapper - New
File Edit View Executable Help
Trace Tree (24617)
CFireWnd::Rand
CFireWnd::BurnPoint
CFireWnd::Rand
CFireWnd::Rand
CFireWnd::Rand
CFireWnd::BurnPoint
CFireWnd::Rand
CFireWnd::Rand
CFireWnd::Rand
CFireWnd::BurnPoint
CFireWnd::Rand
CFireWnd::Rand
CFireWnd::Rand
CFireWnd::BurnPoint
CFireWnd::Rand
CFireWnd::Rand
CFireWnd::Rand
CFireWnd::BurnPoint
330
1202
Process fire.exe:62 exited with code 2
Executable
Name
PID
Status
fire.exe
62
Exited
<New Executable>
Trace Data
CFireWnd::Rand() firewnd.cpp, Line 320
return 61854691
unsigned long = 61854691
Source
void CFireWnd..BurnPoints()
{
CSize size = GetBitmapSize();
BYTE* pRow;
BYTE* pNextRow;
for (int y = m_MaxBurn; y > 0; y--)
{
pRow = (m
pNextRow
Find...
Source Location...
Locate in Trace Options...
)size.cx * 8)
ORD)size.cx
Col 25

FIG. 12

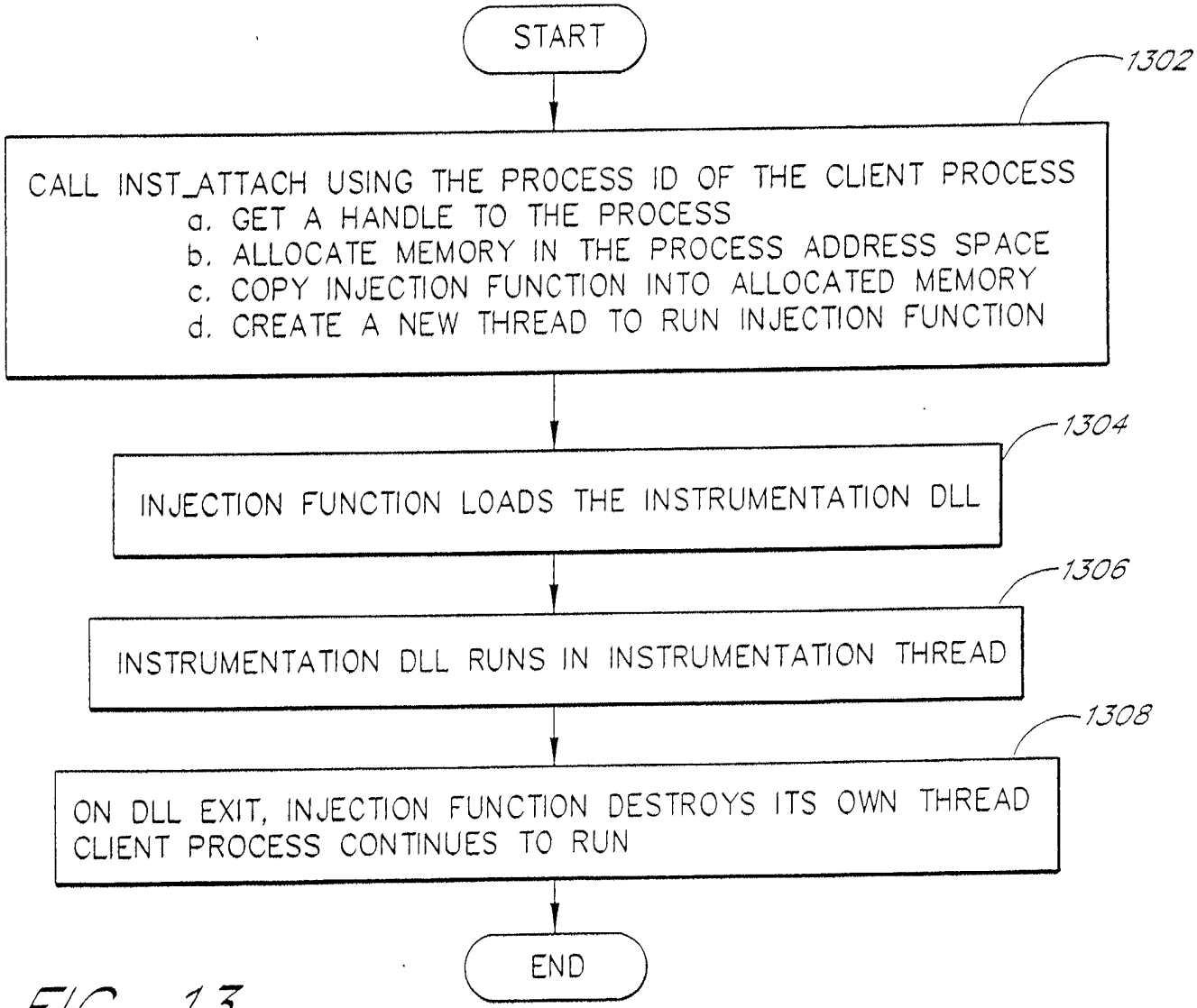

START
1302
CALL INST_ATTACH USING THE PROCESS ID OF THE CLIENT PROCESS
a. GET A HANDLE TO THE PROCESS
b. ALLOCATE MEMORY IN THE PROCESS ADDRESS SPACE
c. COPY INJECTION FUNCTION INTO ALLOCATED MEMORY
d. CREATE A NEW THREAD TO RUN INJECTION FUNCTION
1304
INJECTION FUNCTION LOADS THE INSTRUMENTATION DLL
1306
INSTRUMENTATION DLL RUNS IN INSTRUMENTATION THREAD
1308
ON DLL EXIT, INJECTION FUNCTION DESTROYS ITS OWN THREAD
CLIENT PROCESS CONTINUES TO RUN
END

FIG. 13

Patent Application Publication

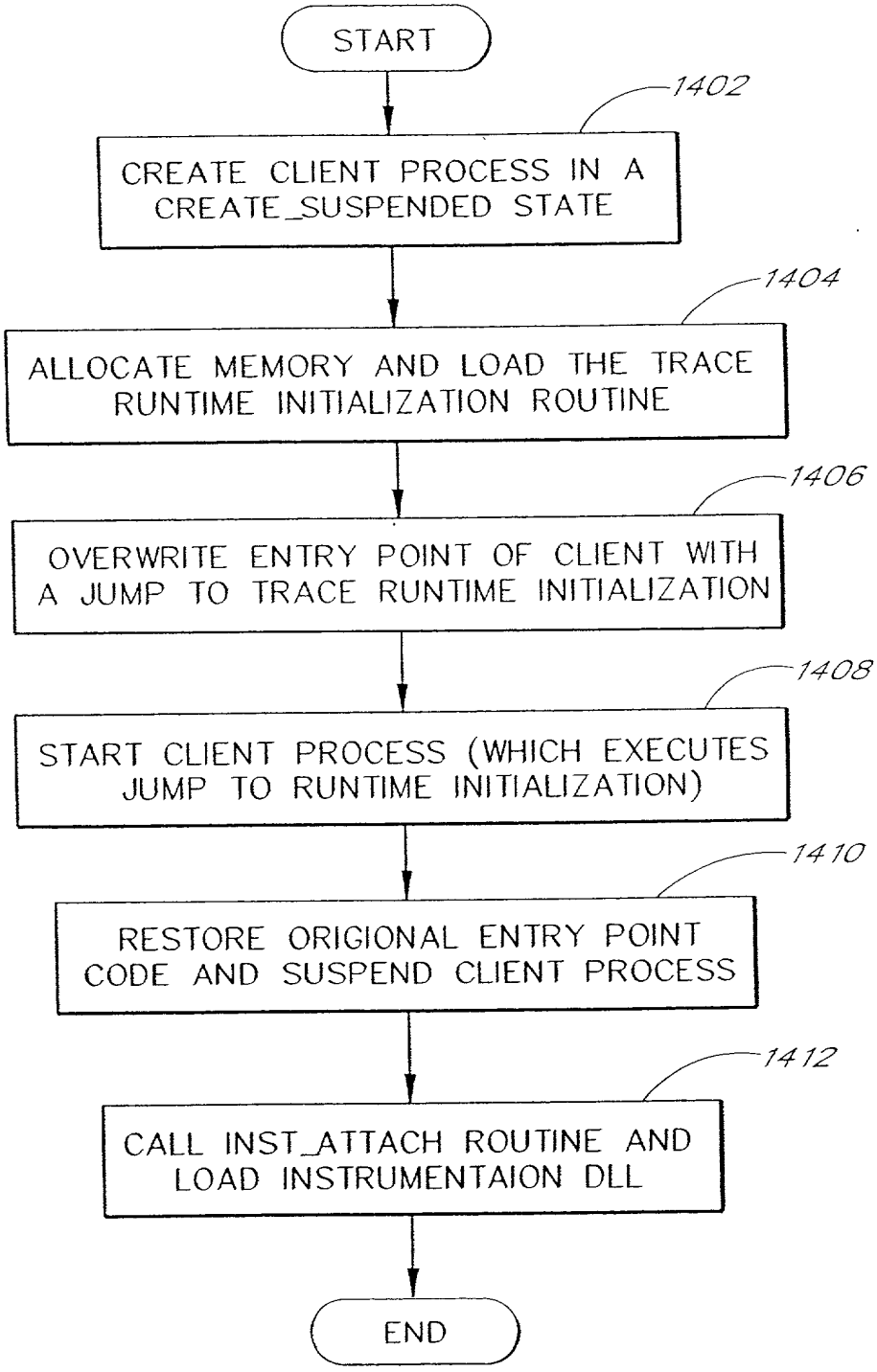


FIG. 14

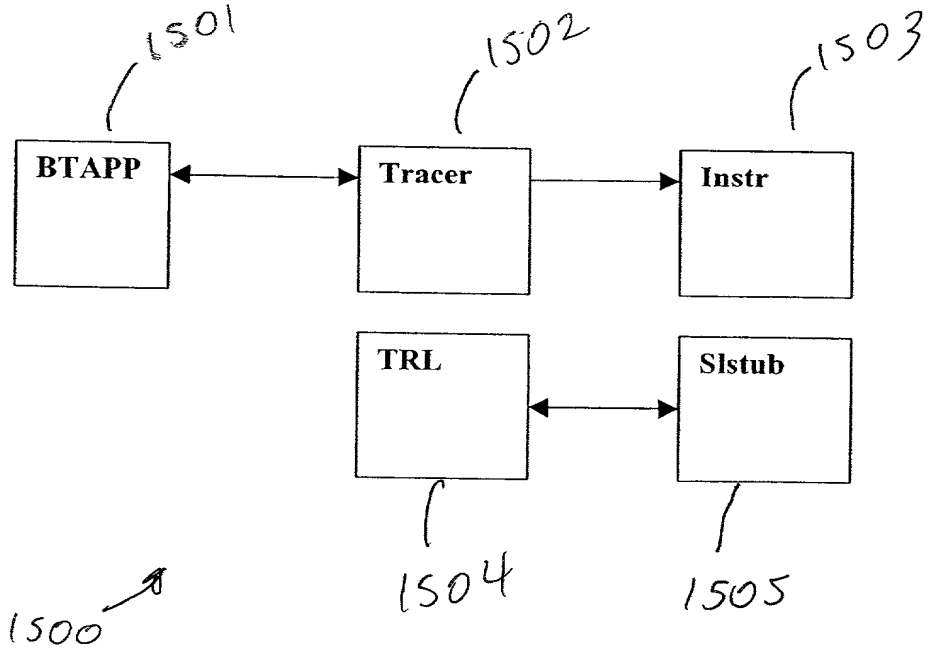


FIG 15

Attorney Docket No. 42390.P13548

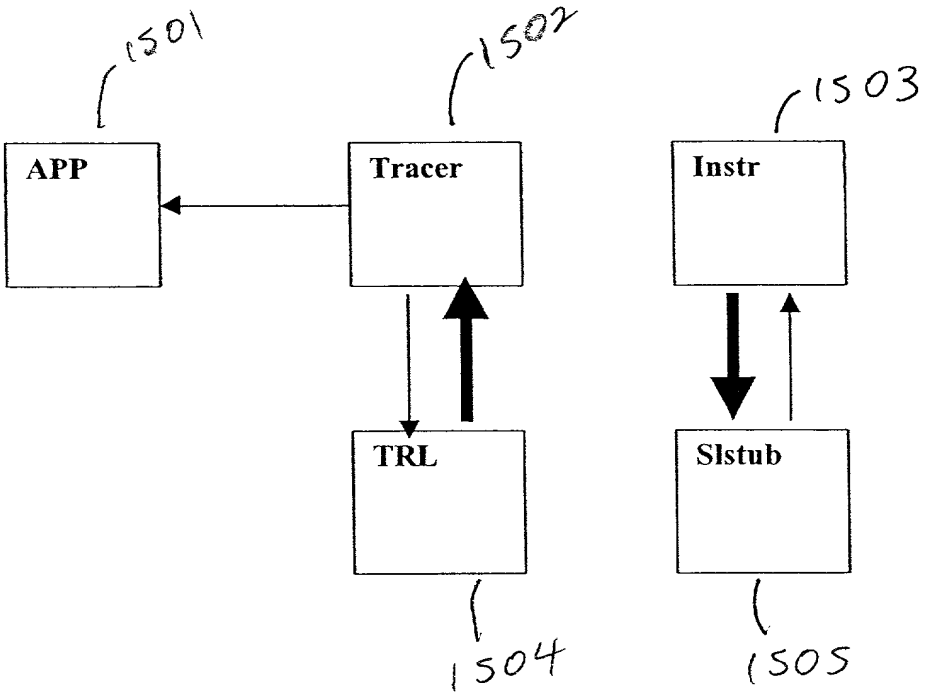


FIG 16

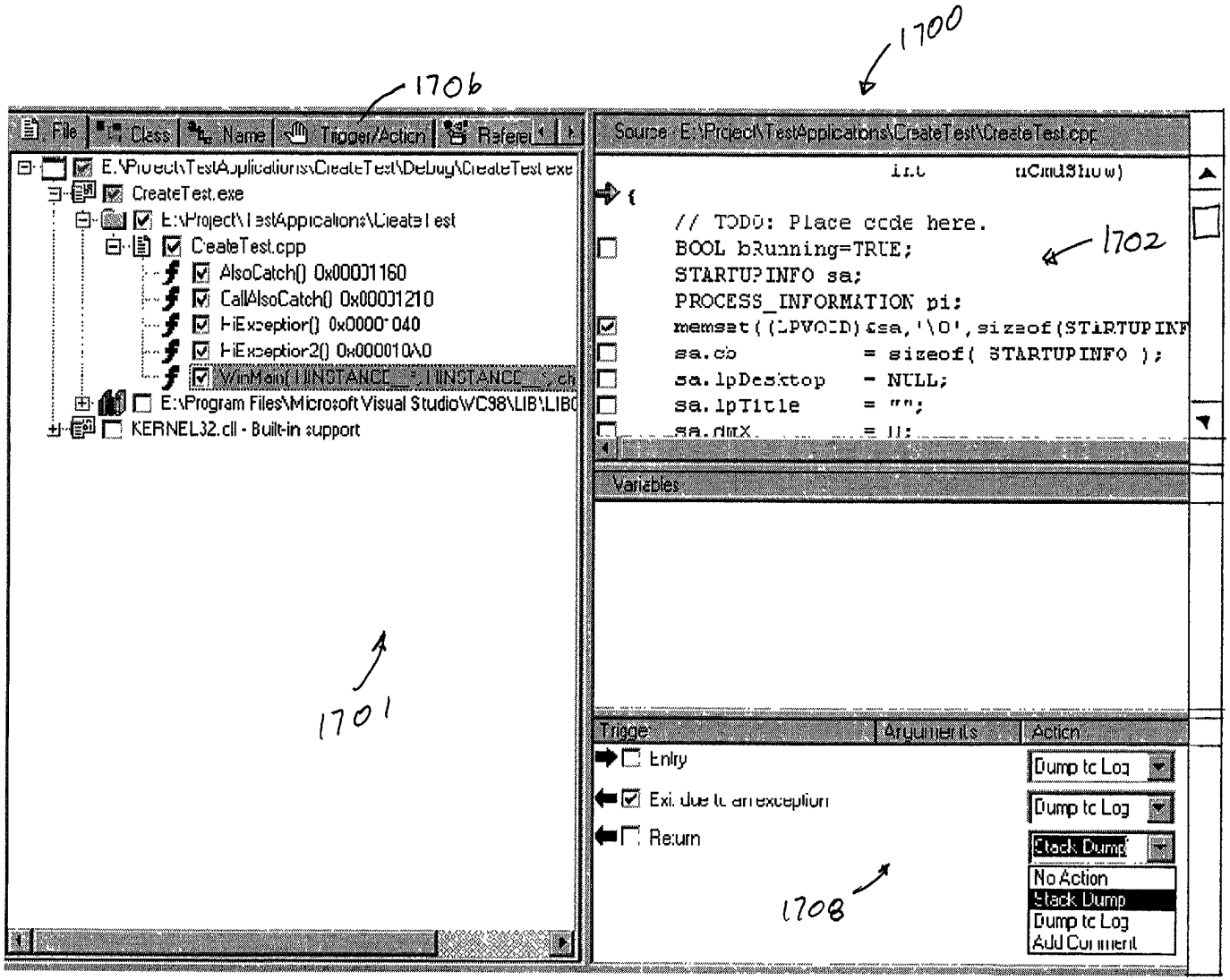

1700
1706
File
Class
Name
Trigger/Action
Source: E:\Project\TestApplications\CreateTest\CreateTest.cpp
E:\Project\TestApplications\CreateTest\Debug\CreateTest.exe
CreateTest.exe
E:\Project\TestApplications\CreateTest
CreateTest.cpp
AlsoCatch() 0x00001160
CallAlsoCatch() 0x00001210
HiException() 0x00001040
HiException2() 0x000010A0
WinMain(HINSTANCE__*,HINSTANCE__*,ch
E:\Program Files\Microsoft Visual Studio\VC98\LIB\LIBC
KERNEL32.dll - Built-in support
// TODO: Place code here.
BOOL bRunning=TRUE;
STARTUPINFO sa;
PROCESS_INFORMATION pi;
memset((LPVOID)&sa,'\0',sizeof(STARTUPINF
sa.cb = sizeof(STARTUPINFO);
sa.lpDesktop = NULL;
sa.lpTitle = "";
1702
Variables
Trigger
Arguments
Action
Entry
Exit due to an exception
Return
Dump to Log
Dump to Log
Stack Dump
No Action
Stack Dump
Dump to Log
Add Comment
1701
1708

FIG 17

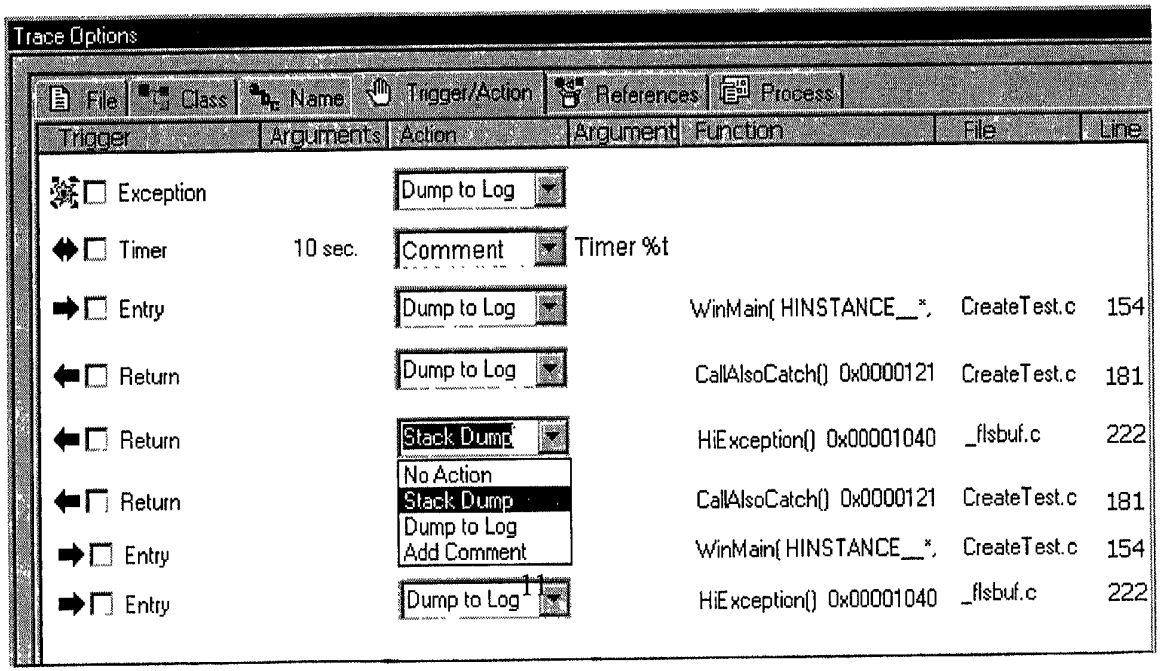

Trace Options
File
Class
Name
Trigger/Action
References
Process
Trigger
Arguments
Action
Argument
Function
File
Line
Exception
Dump to Log
Timer
10 sec.
Comment
Timer %t
Entry
Dump to Log
WinMain(HINSTANCE__*, CreateTest.c 154
Return
Dump to Log
CallAlsoCatch() 0x0000121 CreateTest.c 181
Return
Stack Dump
HiException() 0x00001040 _flsbuf.c 222
No Action
Stack Dump
Dump to Log
Add Comment
Return
CallAlsoCatch() 0x0000121 CreateTest.c 181
Entry
WinMain(HINSTANCE__*, CreateTest.c 154
Entry
Dump to Log
HiException() 0x00001040 _flsbuf.c 222
1800

FIG 18

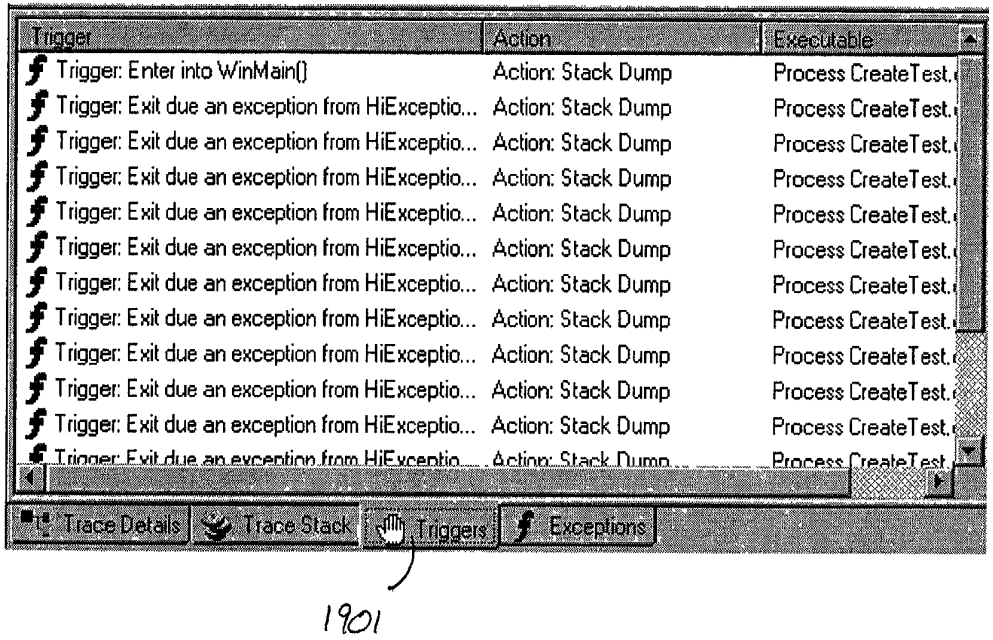
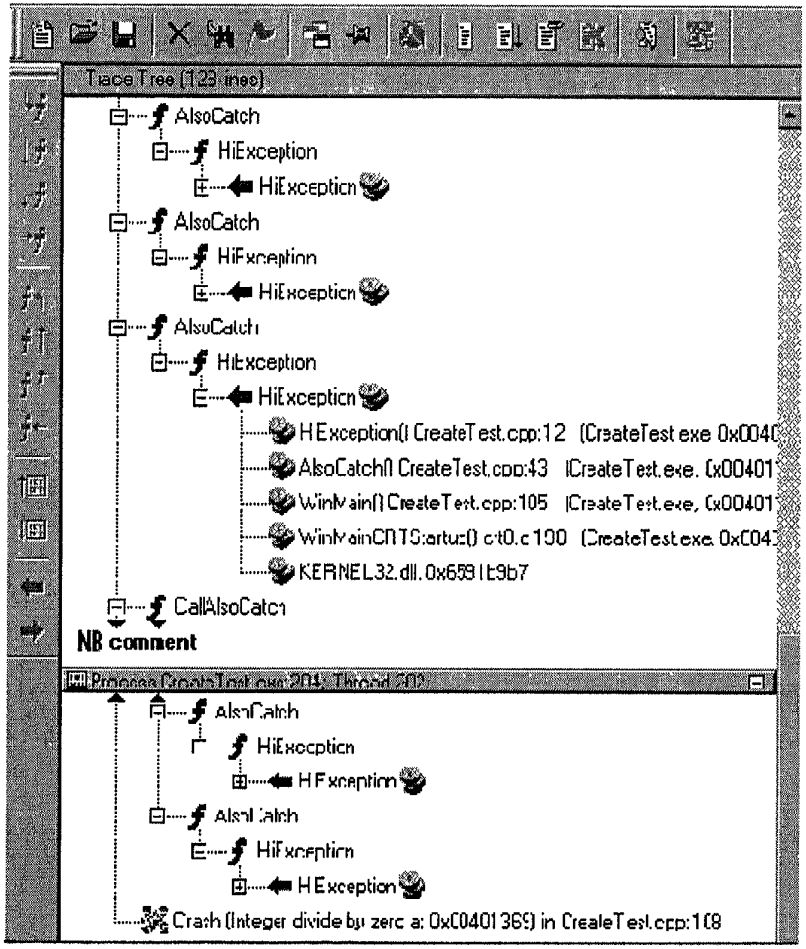

1900
Trigger
Action
Executable
Trigger: Enter into WinMain()
Action: Stack Dump
Process CreateTest.
Trigger: Exit due an exception from HiExceptio...
Action: Stack Dump
Process CreateTest.
Trace Details
Trace Stack
Triggers
Exceptions
1901

FIG 19


Trace Tree (123 lines)
AlsoCatch
HiException
HiException
AlsoCatch
HiException
HiException
AlsoCatch
HiException
HiException
HException() CreateTest.cpp:12 (CreateTest.exe 0x0040
AlsoCatch() CreateTest.cpp:43 (CreateTest.exe, 0x00401
WinMain() CreateTest.cpp:105 (CreateTest.exe, 0x00401
WinMainCRTStartup() crt0.c:100 (CreateTest.exe 0x004
KERNEL32.dll 0x658 1b9b7
CallAlsoCatch
NB comment
AlsoCatch
HiException
HException
AlsoCatch
HiException
HException
Crash (Integer divide by zero at 0x00401369) in CreateTest.cpp:108

2000

FIG 20